I Claim:

Sub a1

1. An electronic mail system, comprising:

a first computer on which is installed message origination software and which is connected to a network capable of carrying an electronic mail message;

at least one recipient computer also connected to said network; and

a viewer applet,

wherein said message origination software is arranged to permit an originator of the electronic mail message to select a date, time, or event, the occurrence of which will cause said electronic mail message and all designated incarnations thereof to expire,

wherein said date, time, or event is attached to the electronic mail message by the message origination software prior to transmission over said network, and

wherein said electronic mail message is encrypted so that it may only be viewed using said viewer applet upon installation of said viewer applet on said at least one recipient computer, whereby upon the occurrence of said date, time, or event, said electronic mail message no longer may be viewed using said viewer applet.

2. An electronic mail system as claimed in claim 1, further comprising a central electronic mail server connected to said network, said message origination software being arranged to send said electronic mail message to said electronic mail server, said electronic mail server being arranged to store said electronic mail message and, upon request by the recipient, encrypt said electronic mail message and stream it to said viewer applet, and said viewer applet being arranged to decrypt said message as it is streamed, so as to display said message.

3. An electronic mail system as claimed in claim 2, wherein said message is encrypted by said central mail server using a public key generated by the viewer applet, said viewer applet being arranged to generate said public key and also a corresponding private key used to decrypt said message.

4. An electronic mail system as claimed in claim 2, wherein said viewer applet is further arranged to permit a user to request forwarding of said electronic mail message stored on said central mail server to a second recipient computer, said central mail server being arranged to encrypt and stream said message to a copy of the viewer applet installed on said second recipient computer and, prior to streaming said message to said second recipient computer, download said viewer applet to said second recipient computer if the viewer applet is not already installed on the second recipient computer.

5. An electronic mail system as claimed in claim 4, wherein said message is encrypted by said central mail server using respective public keys generated by the viewer applet installed on the recipient computer and the copy of the viewer applet installed on the second recipient computer, said viewer applet and said copy of the viewer applet being arranged to generate said respective public keys and also corresponding private keys used to decrypt said message.

6. An electronic mail system as claimed in claim 4, wherein upon the occurrence of said date, time, or event, said central electronic mail server erases said electronic

mail message and, because said electronic mail message is stored only on the central electronic mail server, terminates the existence of the electronic mail message anywhere in this universe.

7. An electronic mail system as claimed in claim 2, wherein upon the occurrence of said date, time, or event, said central electronic mail server erases said electronic mail message and, because said electronic mail message is stored only on the central electronic mail server, terminates the existence of the electronic mail message anywhere in this universe.

8. An electronic mail system as claimed in claim 2, wherein said message origination software is arranged to permit entry of processing and handling limitations, and wherein said processing and handling limitations are attached to said electronic mail message before transmission over said network.

9. An electronic mail system as claimed in claim 8, wherein said processing and handling limitations are implemented by said central server in cooperation with said viewer applet.

10. An electronic mail system as claimed in claim 1, wherein said message is encrypted by a central mail server before transmission to said recipient computer.

11. An electronic mail system as claimed in claim 10, wherein said message is encrypted by said central mail server using a public key generated by the viewer

applet, said viewer applet being arranged to generate said public key and also a corresponding private key used to decrypt said message.

12. An electronic mail system as claimed in claim 1, wherein said message is encrypted by said message origination software using a public key generated by the viewer applet, said viewer applet being arranged to generate said public key and also a corresponding private key used to decrypt said message.

13. An electronic mail system as claimed in claim 1, wherein said viewer applet stores said electronic mail message in encrypted form on said recipient computer and, upon the occurrence of said date, time, or event, erases said electronic mail message.

14. An electronic mail system as claimed in claim 13, wherein said viewer applet is arranged to forward said electronic mail message in encrypted form to a second recipient computer, wherein a copy of said viewer applet is installed on said second recipient computer, and wherein upon the occurrence of said time, date, or event, said copy of the viewer applet erases said electronic mail message.

15. An electronic mail system as claimed in claim 14, wherein said viewer applet is forwarded to said second recipient computer as an attachment to said electronic mail message, thereby causing said system to be self-propagating.

16. An electronic mail system as claimed in claim 1, wherein said message origination software is arranged to permit entry of processing and handling limitations, and wherein said processing and handling limitations are attached to said electronic mail message before transmission over said network.

17. An electronic mail system as claimed in claim 16, wherein said processing and handling limitations are implemented by said viewer applet.

18. A method of controlling an electronic mail message transmitted over a network, comprising the steps of:

before transmission of the electronic mail message over the network, attaching to the message a date, time, or event, the occurrence of which will cause said electronic mail message and all designated incarnations thereof to expire; and

encrypting said electronic mail message so that it can only be viewed before the occurrence of said time, date, or event using a viewer applet installed on a recipient computer.

19. A method of controlling an electronic mail message as claimed in claim 18, further comprising the steps of initially transmitting said electronic mail message over said network to a central electronic mail server, storing said electronic mail message at said electronic mail server and, upon request by the recipient, encrypting said electronic mail message, streaming the encrypted electronic mail message to said viewer applet, and decrypting said electronic mail message as it

is received by the viewer applet so as to display said message without storing it at said recipient computer.

20. A method of controlling an electronic mail message as claimed in claim 19, wherein said step of encrypting said electronic mail message is carried out by said central electronic mail server using a public key generated by the viewer applet, said viewer applet being arranged to generate said public key and also a corresponding private key used to decrypt said message.

21. A method of controlling an electronic mail message as claimed in claim 20, further comprising the steps of causing said viewer applet to request forwarding of said electronic mail message stored on said central mail server to a second recipient computer, encrypting said electronic mail message using a public key of a copy of said viewer applet installed on said second recipient computer, and streaming said electronic message to said second recipient computer.

22. A method of controlling an electronic mail message as claimed in claim 21, wherein upon the occurrence of said date, time, or event, said central electronic mail server erases said electronic mail message and, because said electronic mail message is stored only on the central electronic mail server, terminates the existence of the electronic mail message anywhere in this universe.

23. A method of controlling an electronic mail message as claimed in claim 19, wherein upon the occurrence of said date, time, or event, said central electronic

mail server erases said electronic mail message and, because said electronic mail message is stored only on the central electronic mail server, terminates the existence of the electronic mail message anywhere in this universe.

24. A method of controlling an electronic mail message as claimed in claim 19, further comprising the step of attaching processing and handling limitations to said electronic mail message before transmission over said network.

25. A method of controlling an electronic mail message as claimed in claim 24, further comprising the step of causing said central electronic mail server and viewer applet to implement said processing and handling limitations.

26. A method of controlling an electronic mail message as claimed in claim 18, wherein the step of transmitting said electronic mail message over said network comprises the step of transmitting said message to a central electronic mail server and causing said central electronic mail server to encrypt said message before transmitting it to said recipient computer.

27. A method of controlling an electronic mail message as claimed in claim 26, further comprising the steps of causing said viewer applet to generate a public key and a corresponding private key and transmitting said public key to said central server for use in encrypting said message.

28. A method of controlling an electronic mail message as claimed in claim 18, wherein the step of transmitting said electronic mail message over said network comprises the step of encrypting said message using a public key associated with a private key held by the viewer applet to decrypt said message.

29. A method of controlling an electronic mail message as claimed in claim 28, further comprising the step of causing said viewer applet to store said electronic mail message in encrypted form on said recipient computer and, upon the occurrence of said date, time, or event, erase said electronic mail message.

30. A method of controlling an electronic mail message as claimed in claim 29, further comprising the steps of causing said viewer applet to forward said electronic mail message in encrypted form to a second recipient computer, and upon the occurrence of said time, date, or event, causing a copy of said viewer applet installed on said second recipient computer to erase said electronic mail message.

31. A method of controlling an electronic mail message as claimed in claim 30, further comprising the step of forwarding said copy of the viewer applet to said second recipient computer as an attachment to said electronic mail message, thereby causing said system to be self-propagating.

32. A method of controlling an electronic mail message as claimed in claim 18, further comprising the step of attaching flags indicating processing and handling limitations to said electronic mail message before transmission over said network.

33. A method of controlling an electronic mail message as claimed in claim 32, further comprising the step of causing said viewer applet to implement said processing and handling limitations.

34. An electronic mail system, comprising:

a first computer on which is installed message origination software and which is connected to a network capable of carrying an electronic mail message;

at least one recipient computer also connected to said network;

a viewer applet; and

a central electronic mail server connected to said network, said message origination software being arranged to send said electronic mail message to said electronic mail server, said electronic mail server being arranged to store said electronic mail message and, upon request by the recipient, encrypt said electronic mail message and stream it to said viewer applet, and said viewer applet being arranged to decrypt said viewer applet as it is streamed so as to display said message,

wherein said processing limitations are implemented by said central electronic mail server and said viewer applet.

35. An electronic mail system as claimed in claim 34, wherein said message is encrypted by said central mail server using a public key generated by the viewer applet, said viewer applet being arranged to generate said public key and also a corresponding private key used to decrypt said message.

36. An electronic mail system as claimed in claim 34, wherein said viewer applet is further arranged to permit a user to request forwarding of said electronic mail message stored on said central mail server to a second recipient computer, said central mail server being arranged to encrypt and stream said message to a copy of the viewer applet installed on said second recipient computer and, prior to streaming said message to said second recipient computer, download said viewer applet to said second recipient computer if the viewer applet is not already installed on the second recipient computer.

37. An electronic mail system as claimed in claim 36, wherein said message is encrypted by said central mail server using respective public keys generated by the viewer applet installed on the recipient computer and the copy of the viewer applet installed on the second recipient computer, said viewer applet and said copy of the viewer applet being arranged to generate said respective public keys and also corresponding private keys used to decrypt said message.

38. A method of controlling an electronic mail message transmitted over a network, comprising the steps of:

before transmission of the electronic mail message over the network, attaching limitation on processing and handling of the electronic mail message by a recipient;

initially transmitting said electronic mail message over said network to a central electronic mail server;

storing said electronic mail message at said electronic mail server;

upon request by the recipient, encrypting said electronic mail message, streaming the encrypted electronic mail message to a viewer applet installed on said recipient computer, and decrypting said electronic mail message as it is received by the viewer applet so as to display said message without storing it at said recipient computer; and

causing said central server and viewer applet to implement said processing and handling limitations.

39. A method of controlling an electronic mail message as claimed in claim 38, further comprising the steps of encrypting said electronic mail message is carried out by said central electronic mail server using a public key generated by the viewer applet, said viewer applet being arranged to generate said public key and also a corresponding private key used to decrypt said message.

40. A method of controlling an electronic mail message as claimed in claim 38, further comprising the steps of causing said viewer applet to request forwarding of said electronic mail message stored on said central mail server to a second recipient computer, encrypting said electronic mail message using a public key of a copy of said viewer applet installed on said second recipient computer, and streaming said electronic message to said second recipient computer.

41. A computer program for handling electronic mail, comprising:

a mail origination portion arranged to permit the originator to select a date, time, or event, the occurrence of which will cause said message to expire, said computer

program being arranged to attach said date, time, or event to said electronic mail message before sending of the electronic mail message; and

a viewer applet portion arranged to decrypt a received electronic mail message and to permit viewing of the received electronic mail message before a date, time, or event specified by a sender of the received message.

42. A computer program as claimed in claim 41, wherein said received electronic mail message is encrypted by a central server and streamed to said viewer applet portion, and wherein said viewer applet portion is arranged to decrypt said message as it is streamed from said central server.

43. A computer program as claimed in claim 41, wherein upon the occurrence of said date, time, or event, said viewer applet portion causes said electronic mail message to be erased.

44. A computer program as claimed in claim 41, wherein said message origination program is arranged to attach a copy of said viewer applet portion to each electronic mail message having a specified expiration date, time, or event.

45. A computer program as claimed in claim 41, wherein said message origination program is further arranged to permit the originator to set handling and processing controls, and wherein said viewer applet portion is arranged to implement handling and processing controls on a received message.

46. A method of distributing applets for viewing electronic files, comprising the steps of:

encrypting the electronic files so that they can only be viewed by the viewer applet;

transmitting the encrypted electronic file from a computer of an originator of the file to a computer of a recipient designated by the originator;

if the computer of the recipient does not have said viewer applet installed thereon, transmitting said viewer applet to the computer of the recipient either before or simultaneously with the transmission of the electronic file.

47. A method as claimed in claim 46, further comprising the step of notifying the recipient that an encrypted electronic file has been received and that the electronic file can only be viewed upon installation of said viewer applet on the computer of the recipient.

48. A method as claimed in claim 47, wherein the step of notifying the recipient is carried out by a central server, said central server also supplying said viewer applet to said computer of the recipient.

49. A method as claimed in claim 46, wherein the viewer applet is transmitted simultaneously with the electronic file from the computer of the originator to the computer of the recipient.

50. A method as claimed in claim 46, wherein the electronic file is an electronic mail message, and the viewer applet is transmitted as an attachment to the electronic mail message.